PCT/GB 99/02673

12 AUGUST 1999

#7

INVESTOR IN PEOPLE

4

GB99/2673

The Patent Office

PRIORITY DOCUMENT

SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

REC'D 29 SEP 1999
WIPO PCT

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

I also certify that the attached copy of the request for grant of a Patent (Form 1/77) bears a correction, effected by this office, following a request by the applicant and agreed to by the Comptroller-General.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

Signed

Dated 16 AUG 1999

Patents Form 1/77

Act 1977
(Rule 16)

THE PATENT OFFICE
20 AUG 1998
NEWPORT
RECEIVED BY POST

The Patent Office

20 AUG 1998
21AUG98 E584808-3 D02846
P01/7700 25.00 - 9818187.8

Request for grant of a patent

(See the notes on the back of this form. You can also g an explanatory leaflet from the Patent Office to help you fill in this form)

9818187.8

The Patent Office

Cardiff Road
Newport
Gwent NP9 1RH

1. Your reference — PLB/CC/N872

2. Patent application number
(The Patent Office will fill in this part)

3. Full name, address and postcode of the or of each applicant *(underline all surnames)*

~~UNDERSHAW GLOBAL LIMITED~~
TRIDENT CHAMBERS
PO BOX 146
WICKHAMS CAY
ROAD TOWN
TORTOLA
~~BRITISH VIRGIN ISLANDS~~

Comodo Technology Development Limited
The Fold, 3 City Road
HALIFAX
UK

Patents ADP number *(if you know it)* ~~07594257001~~

If the applicant is a corporate body, give the country/state of its incorporation ~~BRITISH VIRGIN ISLANDS~~

4. Title of the invention

IMPROVEMENTS IN AND RELATING TO ACCESS CONTROL

5. Name of your agent *(if you have one)*

APPLEYARD LEES

"Address for service" in the United Kingdom to which all correspondence should be sent *(including the postcode)*

15 CLARE ROAD
HALIFAX
WEST YORKSHIRE
HX1 2HY

Patents ADP number *(if you know it)* ~~AA005~~ 190001

6. If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and *(if you know it)* the or each application number	Country	Priority application number *(if you know it)*	Date of filing *(day / month / year)*

7. If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application	Number of earlier application	Date of filing *(day / month / year)*

8. Is a statement of inventorship and of right to grant of a patent required in support of this request? *(Answer 'Yes' if:*

a) any applicant named in part 3 is not an inventor, or
b) there is an inventor who is not named as an applicant, or
c) any named applicant is a corporate body.
See note (d))

YES

Patents Form 1/77

9. Enter the number of sheets for any of the following items you are filing with this form. Do not count copies of the same document

Continuation sheets of this form	
Description	7 x 2
Claim(s)	
Abstract	
Drawing(s)	2 x 2

10. If you are also filing any of the following, state how many against each item.

Priority documents	
Translations of priority documents	
Statement of inventorship and right to grant of a patent *(Patents Form 7/77)*	
Request for preliminary examination and search *(Patents Form 9/77)*	
Request for substantive examination *(Patents Form 10/77)*	
Any other documents *(please specify)*	

11. I/We request the grant of a patent on the basis of this application.

Signature Aylward Lees Date 19 AUGUST 1998

12. Name and daytime telephone number of person to contact in the United Kingdom

PAUL BRANDON
0161 228 0903

Warning

After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.

Notes

a) If you need help to fill in this form or you have any questions, please contact the Patent Office on 0645 500505.

b) Write your answers in capital letters using black ink or you may type them.

c) If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.

d) If you have answered 'Yes' Patents Form 7/77 will need to be filed.

e) Once you have filled in the form you must remember to sign and date it.

f) For details of the fee and ways to pay please contact the Patent Office.

IMPROVEMENTS IN AND RELATING TO ACCESS CONTROL

Field of the Invention

The present invention relates to access control devices and methods.

Background to the Invention

Password protection is often used to control access to data or software as a result of which considerable attention has been paid to the breaking of password protection.

Referring to Figure 1 of the drawings that follow, there is shown a representative flow diagram of a prior art password protection method, according to which a corresponding device operates. In the Figures the abbreviation "PW" is used for "password".

At 100 a selected password is entered. The password may be user-selected or allocated in some other way.

The selected password is stored (102) at a memory location within the device. The device then enters its normal operation (104) as part of which it determines as each access request is submitted whether this is a password protected access (106). If it is not a password protected access, the "NO" branch is followed and normal operation resumes. If it is a password protected access, the "YES" branch is followed and a password is requested (108). Upon input of a password, the input password is compared (110) with the password stored at a memory location. If the input password is the same as the stored password (112) the "YES" branch is followed and normal

operation resumes (104). Otherwise, the "NO" branch is followed and access is denied (114). As is well known in the art, instead of denying access upon the first input of an erroneous password, a further try or several further tries may be permitted up to a predetermined number of attempts with an incremented tamper count upon each failed password entry. In addition to denying access, alerts or alarms may be activated.

In the method and corresponding device described above, since the usual implementation is upon a digital computer, a de-bug program can be run alongside the password protection. As part of which, the de-bug program can, upon entry of any password, follow the program to the memory location at which the correct password is stored for comparison purposes. The de-bug program can then be used to copy the stored password from that memory location for correct entry. In this way, the prior art method and corresponding device described above is vulnerable to attack and to the bypass of the password security even if the data is encrypted.

It is an aim of preferred embodiments of the present invention to obviate or overcome at least one disadvantage encountered in relation to the prior art, whether referred to herein or otherwise.

Summary of the Invention

According to the present invention in a first aspect there is provided an access control device comprising means for receiving an input password, means for combining the input password with a pre-selected code thereby to produce a combined password, and means for decrypting encrypted code using the combined password.

Suitably, the apparatus further comprises means for encrypting the combined password and the encrypted combined password is used for decryption.

According to the present invention in a second aspect, there is provided a method of controlling access, which method comprises the steps of receiving an input password, combining the input password with a predetermined code to produce a combined password, and decrypting encrypted code using the combined password.

Suitably, the combined password is encrypted and the encrypted combined password is used for decrypting encrypted code.

Suitably, the encrypted combined password is a key for decryption of the encrypted code.

Suitably, the password is an alphanumeric string. Suitably, the code is an alphanumeric string.

Suitably, the pre-stored access password comprises a pre-selected password combined with the predetermined code, which combination is encrypted.

Normally the combined pre-selected password is encrypted according to the encryption algorithm used for the combined password. Suitably, the encryption is substantially unreversible. Typically, the encryption algorithm will be a public key algorithm.

Brief Description of the Figures

The present invention will now be described, by way of example only, with reference to the drawings that follow; in which:

Figure 1 is a representative flow diagram of a prior art access control method.

Figure 2 is a representative functional flow diagram of an access control method according to the present invention.

Description of the Preferred Embodiments

Referring to Figure 2 of the drawings that follow, there is shown a flow diagram illustrating a method according to the present invention, according to which method a corresponding device may operate.

At 200 a password is selected. As with the prior device and method, the password may be user-selected or chosen in some other way.

The selected password is then combined with (202) with a longer password string at pre-selected locations therewithin. This produces a combined password which is encoded (204). Normally, the encoding step will comprise a public key, substantially irreversible, encryption, but in theory could be as simple as carrying out an AND or XOR operation.

The encrypted combined password is used as an encryption key to encrypt data (206) which may be software. Notably, the encrypted combined password is not stored in any memory location. Following this the device enters normal operation (208) as part of which it checks

(210) whether a requested data/software access is password protected. If the access is not password protected the "NO" branch is followed back to normal operation. Otherwise, the "YES" branch is followed and a request is made for a password to be input (212). Upon input of a password, it is inserted into pre-selected locations of the predetermined string (214). This is the same predetermined string with which the original password is combined (202). This produces a combined password which is encrypted at (216) using the same encryption as at 204.

The encrypted combined password is used as a decryption key to decrypt the encrypted data/software to which access is sought. Therefore only entry of a correct password will properly decrypt the data/software.

By way of example, therefore, at step 200, the password "FRED" may be entered by a user. The selected password is combined with the string A7BX2Q66FEAR3YD at locations subsequent to characters 2, 6, 9 and 13 (by order). This produces (202) the following combined result: A7FBXS2RQ66EFEARD3YD. The underlined letters are the password letters inserted at pre-selected points within the longer string. They are underlined for the purposes of explanation only.

At step 204, the combined password is encrypted according to any encryption method. Preferably, a public key encryption is used but this need not be the case. This may result in an output as follows: 3XTAV2?8BAD99X. The encrypted result need not be the same length as the combined password. The encrypted combined password is then used as an encryption key to encrypt data or software. If password protected access is sought (210), an input password is requested (212). Here, if an

incorrect password is entered, for instance "MOUSE" it will be combined (214) with the pre-selected string at the pre-selected locations to give the following result A7MBXS2OQ66UFEARS3YED. This combined input password is then encrypted (216) according to the same encryption used at step 204 and used as a decryption key to decrypt the encrypted data. As the key is wrong the decryption will be inaccurate.

In the case of the correct password "FRED" being input at 212, it will be inserted at corresponding locations encrypted and will correspond to the key used for encryption. Thus when used as a decryption key it will accurately decrypt the data.

Accordingly, neither the password to be used by the user nor the decryption key is not stored anywhere within the device. Thus, by inspection of the device running a for instance, de-bug program, an unauthorised user would not be able to gain access to the necessary password nor to the decryption key.

Although reference is made herein to "passwords" it will be appreciated that this could be any signal or combination of signals and need not be a word at all.

A device operating as set out above with reference to preferred embodiments of the invention may be embodied in a digital computer or otherwise.

The reader's attention is directed to all papers and documents which are filed concurrently with or previous to this specification in connection with this application and which are open to public inspection with

this specification, and the contents of all such papers and documents are incorporated herein by reference.

All of the features disclosed in this specification (including any accompanying claims, abstract and drawings), and/or all of the steps of any method or process so disclosed, may be combined in any combination, except combinations where at least some of such features and/or steps are mutually exclusive.

Each feature disclosed in this specification (including any accompanying claims, abstract and drawings), may be replaced by alternative features serving the same, equivalent or similar purpose, unless expressly stated otherwise. Thus, unless expressly stated otherwise, each feature disclosed is one example only of a generic series of equivalent or similar features.

The invention is not restricted to the details of the foregoing embodiment(s). The invention extends to any novel one, or any novel combination, of the features disclosed in this specification (including any accompanying claims, abstract and drawings), or to any novel one, or any novel combination, of the steps of any method or process so disclosed.

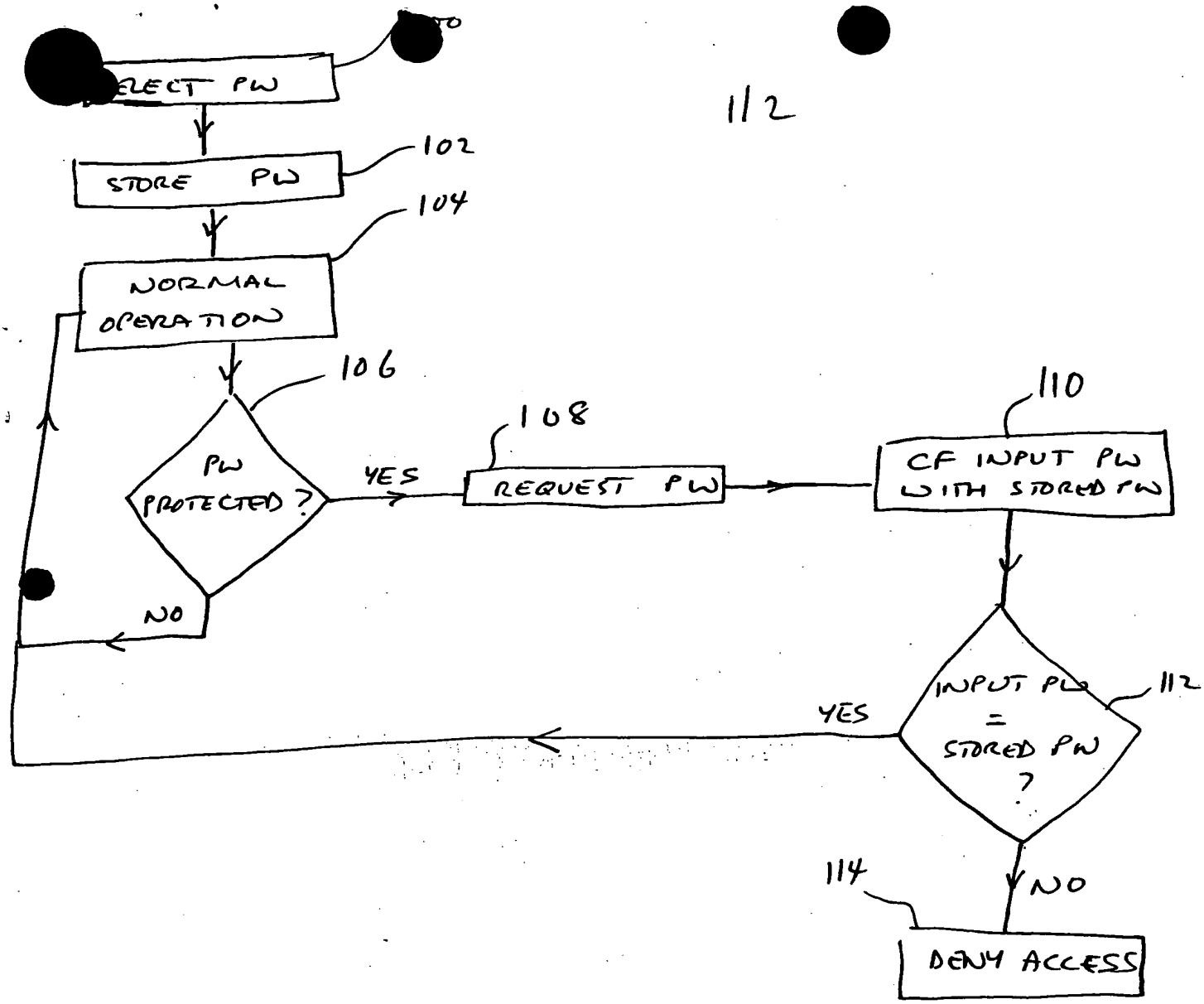
ELECT PW
STORE PW
102
NORMAL OPERATION
104
106
PW PROTECTED?
YES
NO
108
REQUEST PW
110
CF INPUT PW WITH STORED PW
INPUT PW = STORED PW ?
112
YES
NO
114
DENY ACCESS

FIGURE 1

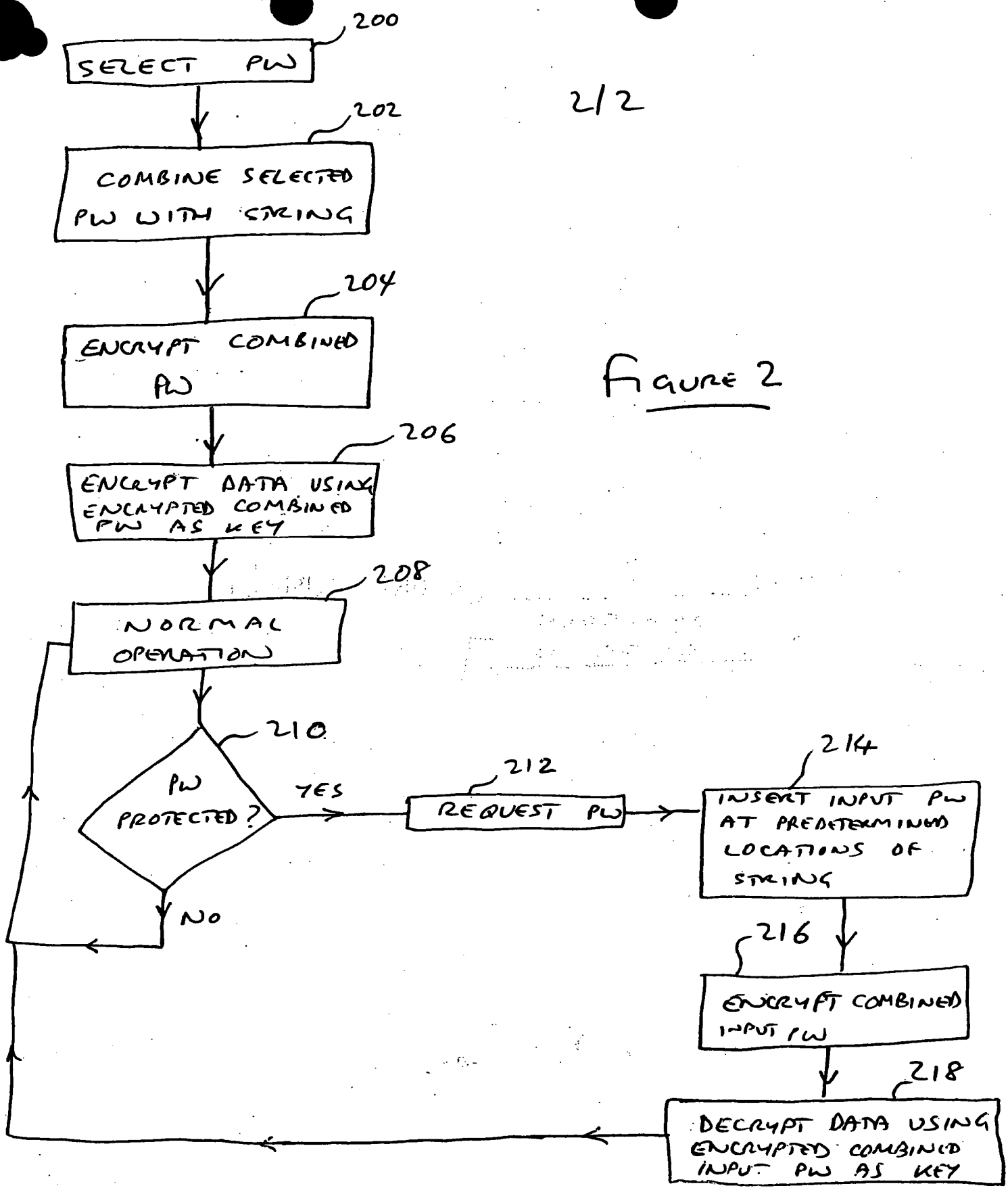
200
SELECT PW
202
COMBINE SELECTED PW WITH STRING
204
ENCRYPT COMBINED PW
206
ENCRYPT DATA USING ENCRYPTED COMBINED PW AS KEY
208
NORMAL OPERATION
210
PW PROTECTED?
YES
NO
212
REQUEST PW
214
INSERT INPUT PW AT PREDETERMINED LOCATIONS OF STRING
216
ENCRYPT COMBINED INPUT PW
218
DECRYPT DATA USING ENCRYPTED COMBINED INPUT PW AS KEY

Figure 2